Theorem of Numbers homework 7
Euler’s phi function, Euler’s theorem
Due November 5th, 2018

In all what follows, \( \phi \) denotes Euler’s phi function. You must give details of all calculations.

**Exercise 1.** Establish each of the assertions below:

1. If \( n \) is an odd integer, then \( \phi(2n) = \phi(n) \).
   
   *Solution.* If \( n \) is odd, then \( n \) is relatively prime to 2, so by multiplicativity, we have \( \phi(2n) = \phi(2)\phi(n) = \phi(n) \) since \( \phi(2) = 1 \).

2. \( \phi(3n) = 2\phi(n) \) if and only if 3 does not divide \( n \).
   
   *Solution.* We may write \( n \) in the form \( n = 3^km \) where \( k \geq 0 \) (\( k = v_3(n) \) is allowed to be zero: this is the case when \( n \) is not divisible by 3 and \( m \) is not divisible by 3. Then by multiplicativity, \( \phi(3n) = \phi(3^{k+1})\phi(m) = 3^k \times 2 \times \phi(m) \), whereas
   
   \[
   \phi(n) = \phi(3^k)\phi(m) = \begin{cases} 
   3^{k-1} \times 2 \times \phi(m) & \text{if } k \geq 1 \\
   \phi(m) & \text{if } k = 0
   \end{cases}
   \]

   Thus, \( \phi(3n) = 3\phi(n) \) if \( 3|n \) and \( \phi(3n) = 2\phi(n) \) otherwise. In particular, since \( \phi(n) \) is non-zero, \( \phi(3n) = 2\phi(n) \) if and only if \( n \) is not divisible by 3.

3. \( \phi(n) = \frac{n}{2} \) if and only if \( n = 2^k \) for some \( k \geq 1 \).
   
   *Solution.* Assume \( \phi(n) = \frac{n}{2} \). First of all, since \( \phi(n) \) is an integer, this means that \( n \) is even, so we may write \( n = 2^km \) where \( m \) is odd and \( k = v_2(n) \geq 1 \). Then
   
   \[
   \phi(n) = \phi(2^k)\phi(m) = 2^{k-1}\phi(m),
   \]

   so that our assumption implies \( 2^{k-1}\phi(m) = \frac{3^k-1}{2}m \), whence we have \( \phi(m) = m \). This clearly implies \( m = 1 \), and so \( n = 2^k \). Conversely, if \( n = 2^k \) with \( k \geq 1 \), we have \( \phi(n) = 2^k - 1 = \frac{n}{2} \).

**Exercise 2.** Show that there are infinitely may integers \( n \) such that \( \phi(n) = \frac{n}{3} \).

*Solution.* Look at the integers of the form \( 3 \times 2^k \) for \( k \geq 1 \). We have

\[
\phi(3 \times 2^k) = \phi(3)\phi(2^k) = 2 \times 2^{k-1} = 2^k.
\]

Note that in fact, for the same reason, all integers of the form \( 2^k3^j \) where \( k, j \geq 1 \), work.

**Exercise 3.** Describe the integers \( n \) such that \( \phi(n) \) is not divisible by 4.

*Solution.* First of all, note that if \( n = p^k \) is a prime power with \( p \) odd, then \( \phi(p^k) = p^{k-1}(p-1) \) is even because \( p-1 \) is even. Moreover, since \( p^{k-1} \) is odd, it is divisible by 4 if and only if \( p-1 \) is divisible by 4, that is, if and only if \( p \equiv 1 \pmod{4} \). If \( n = 2^k \), then \( \phi(n) = 2^{k-1} \) is even if \( k \geq 2 \) and divisible by 4 if \( k \geq 3 \).

We know that if \( n \) has prime factorization \( n = p_1^{k_1} \ldots p_r^{k_r} \) for positive \( k_1, \ldots, k_r \) and distinct primes \( p_1, \ldots, p_r \), then

\[
\phi(n) = \phi(p_1^{k_1}) \ldots \phi(p_r^{k_r}).
\]

Because of the above observation, \( \phi(n) \) will be divisible by 4 as soon as one of its prime factors is congruent to 1 modulo 4. Assume now that \( n \) has no prime factors congruent to 1 modulo 4.
If \( n \) is odd, then by the above observation, all of the \( \phi(p^k) \) are even, and \( \phi(n) \) is divisible by 4 as soon as \( r \geq 2 \). If \( r = 1 \), then \( n \) is the power of a prime congruent to 3 modulo 4, so \( \phi(n) \) is not divisible by 4.

Assume now \( n \) is even, so that we may assume \( p_1 = 2 \). If \( r \geq 3 \) (that is, if \( n \) has another two prime factors) then \( \phi(n) \) is divisible by 4 by the above. If \( r = 2 \), that is, if \( n \) has exactly one other prime factor \( p_2 \) (which is congruent to 3 modulo 4), then, for \( \phi(n) \) to be not divisible by 4, we need \( \phi(2^{k_1}) \) to be not divisible by 2, so \( k_1 = 1 \). If \( r = 1 \) (that is, if \( n \) is a power of 2), then by the above, we need \( k_1 = 1 \) or 2 (that is, \( n = 2 \) or \( n = 4 \)).

As a conclusion, the integers \( n \) such that \( \phi(n) \) is not divisible by 4 are exactly those of the form \( p^k \) or \( 2p^k \) where \( p \) is a prime congruent to 3 modulo 4 and \( k \geq 1 \), as well as 2 and 4.

**Exercise 4.** Find the remainder of \( 11^{1213} \) in the Euclidean division by 26.

*Solution.* We have \( \phi(26) = \phi(2)\phi(13) = 12 \), so by Euler’s theorem, since 11 is relatively prime to 26,

\[
11^{12} \equiv 1 \pmod{26}.
\]

Now, \( 1213 \equiv 1 \pmod{12} \), so \( 11^{1213} \equiv 11 \pmod{26} \).

**Exercise 5.** Find the last two digits of \( 2^{2018} \).

*Solution.* The last two digits are detected by looking modulo 100. However 2 and 100 have a common factor, so we cannot apply Euler’s theorem directly. Since 100 = \( 4 \times 25 \), and 2 is relatively prime to 25, let’s apply Euler’s theorem modulo 25: we have \( \phi(25) = \phi(5^2) = 5^2 - 5 = 20 \), so

\[
2^{20} \equiv 1 \pmod{25}.
\]

Since \( 2020 \) is divisible by 20, we get

\[
2^{2020} \equiv 1 \pmod{25}.
\]

Now, 13 is an inverse of 2 modulo 25, so multiplying by \( 13^2 \) we get

\[
2^{2018} \equiv 13^2 \equiv 19 \pmod{25}.
\]

A number congruent to 19 modulo 25 must have his two last digits equal to 19, \( 19 + 25 = 44 \) or \( 19 + 3 \times 25 = 94 \). Since we moreover know that \( 2^{2018} \) is divisible by 4, we get that its two last digits are 44.

**Exercise 6.** You want to do RSA cryptography with \( n = pq \) where \( p = 11 \) and \( q = 13 \).

1. What is the smallest possible value of the encode exponent \( e \) that you can choose?

   *Solution.* We have \( \phi(n) = 10 \times 12 = 120 \). We need \( e \) to be greater than 1 and relatively prime to \( \phi(n) \), so the smallest possible value is \( e = 7 \).

2. Taking \( e \) to be equal to this value, compute a decode exponent \( d \).

   *Solution.* The integer \( d \) must be an inverse of \( e = 7 \) modulo 120. Note that

   \[
   7 \times 17 = 119 \equiv -1 \pmod{120},
   \]

   so \( 7 \times 103 \equiv 7 \times (-17) \equiv 1 \pmod{120} \), so \( d = 103 \) works.
3. Bob wants to let Alice know on which day in October your Theory of Numbers midterm is. What message will he be sending to Alice?

Solution. You want to send the number 29. The computation goes for example as follows:

\[ 29^2 = 841 \equiv 126 \equiv -17 \pmod{143} \]

so squaring everything,

\[ 29^4 \equiv (-17)^2 \equiv 3 \pmod{143}. \]

Thus, \( 29^7 = 29^4 \times 29^2 \times 29 \equiv 3 \times (-17) \times 29 = -1479 \equiv -49 \equiv 94 \pmod{143} \). So Bob must send the number 94 to Alice.